Receipt

PATENTS

IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Christopher D. Blair

Art Unit: **2681**

Confirmation No.: 4998

Serial No: **10/525,260**

Docket No.: **762301-1560**

Filed: **February 22 2005**

For: **Method and System for Communications Monitoring**

REQUEST FOR CORRECTION TO THE FILING RECEIPT

Commissioner for Patents
ATTN: Office of Initial Patent Examination
Customer Service Center
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Applicant hereby advises the Commissioner that David Alan Gill is listed as an Applicant. Mr. Gill was the agent of record when the Application under the PCT (PCT/GB02003/003668; filing date August 21, 2003) was filed, and not an Applicant. A copy of the PCT Application is attached to this Request for Correction to the Filing Receipt. Therefore, Applicant hereby requests that David Alan Gill, London, United Kingdom, be removed as an Applicant in this Application, and that a Corrected Filing Receipt be issued to the undersigned attorney.

Respectfully submitted,

M. Paul Qualey, Jr.
Attorney for Applicant

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.
100 Galleria Parkway, Suite 1750
Atlanta, Georgia 30339-5948

Date: 04/12/06
Customer No.: 24504

CERTIFICATE OF MAILING

I hereby certify that the below-listed are being deposited with the U.S. Postal Service as first class mail in an envelope addressed to:

Mail Stop Office of Initial Patent Examination
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

on 04/12/06.

Anne Antonoff

In re application of:

Christopher D. Blair Art Unit: **2681**

Serial No: **10/525,260**

Filed: **March 22, 2005** Docket No.: **762301-1560**

For: **Method and System for Communication Monitoring**

The following is a list of documents enclosed:

Return Postcard
Request for Correction of Filing Receipt
Copy of Original Filing Receipt
Copy of PCT Application PCT/GB2003/003668

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPL NO.	FILING OR 371 (c) DATE	ART UNIT	FIL FEE REC'D	ATTY.DOCKET NO	DRAWINGS	TOT CLMS	IND CLMS
10/525,260	02/22/2005	2681	1400	091608.00005	1	22	5

CONFIRMATION NO. 4998

Stefan V Stein
Holland & Knight
P O Box 1288
Tampa, FL 33601-1288

FILING RECEIPT

OC000000018168623

Date Mailed: 03/21/2006

Receipt is acknowledged of this regular Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Christopher Douglas Blair, East Sussex, UNITED KINGDOM;
David Alan Gill, London, UNITED KINGDOM;

Power of Attorney:

Stefan Stein--29702

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/GB03/03668 08/21/2003

Foreign Applications

UNITED KINGDOM 0219493.4 08/21/2002

If Required, Foreign Filing License Granted: 03/01/2006

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is US10/525,260

Projected Publication Date: 06/08/2006

Non-Publication Request: No

Early Publication Request: No

Title

Method and system for communications monitoring

Preliminary Class

455

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 March 2004 (04.03.2004)

PCT

(10) International Publication Number
WO 2004/019585 A1

(51) International Patent Classification[7]: H04L 29/06, G06F 1/00, H04M 3/22

(21) International Application Number: PCT/GB2003/003668

(22) International Filing Date: 21 August 2003 (21.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0219493.4 21 August 2002 (21.08.2002) GB

(71) Applicant *(for all designated States except US)*: EYRE-TEL plc [GB/GB]; Kings Court, Kingston Road, Leatherhead, Surrey KT22 7SZ (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: BLAIR, Christopher, Douglas [GB/GB]; Ivor Cottage, South Chailey, Lewes, East Sussex BN8 4AP (GB).

(74) Agent: GILL, David, Alan; W.P. Thompson & Co., 55 Drury Lane, London WC2B 5SQ (GB).

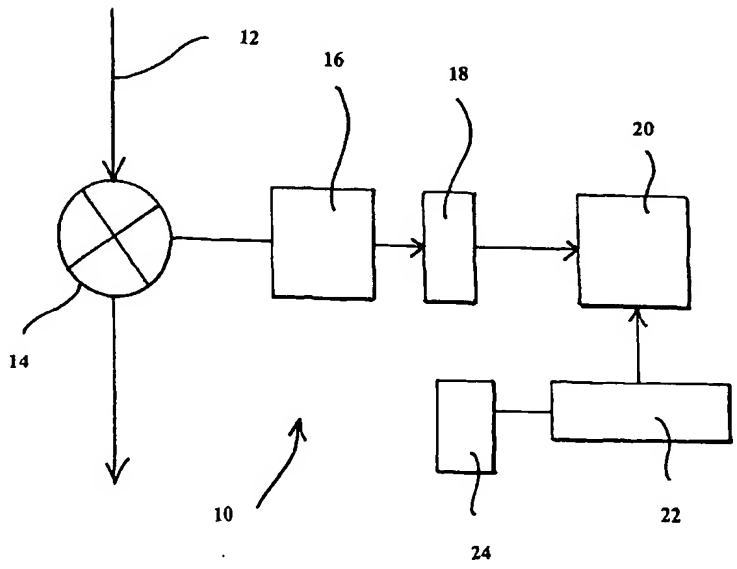
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR COMMUNICATIONS MONITORING



(57) Abstract: The present invention provides for a system, and related method, for use in the monitoring of communications traffic, comprising the step of recording the said traffic and storing the recorded traffic in an encrypted data format such that the data can be decrypted only by means of keys that exhibit restricted availability.

WO 2004/019585 A1

METHOD AND SYSTEM FOR COMMUNICATIONS MONITORING

The present invention relates to a method and system for communications monitoring and, in particular, to a method and system for use in the surveillance of communications traffic.

With the increase in commercial transactions conducted via the internet, or via a telephone call, commercial organisations have increasingly turned to recording technology to assist with monitoring the performance of their customer service employees who, quite commonly, might be located within a call centre designed specifically to handle a large number and variety of telephone enquires and transactions. It is therefore now quite common for such transactions to be monitored and prior warnings are given providing a customer with a clear indication that the conversation may be recorded for training and quality-control purposes. The recording of such transactions can also prove to be of assistance in meeting regularity requirements and enhancing the possibilities for dispute resolution.

The employment of such recording techniques has however remained very much in the commercial environment since the indiscriminate recording of, for example, telephone communications traffic in general, and including mere public communications traffic, carries with it far greater data protection and privacy issues.

Although it is known for law enforcement agencies to obtain authorisation to place wire-taps in order to monitor, for example, telephone communications involving a likely criminal source, such authorisation is granted only once particular criteria concerning the level of suspicion of the criminal source are met: which, of course somewhat disadvantageously can often prove to be after incriminating communications traffic has already been sent.

The present invention seeks to overcome such disadvantages with regard to the time-lag that can currently exist when seeking to monitor communications traffic and with regard to the likely occurrence of potentially incriminating traffic and the initiation of a monitoring/surveillance program.

According to a first aspect of the present invention, there is provided a method for use in the monitoring of communications traffic, and comprising the steps of recording the said traffic, storing the recorded traffic in an encrypted data format and such that this data can be decrypted only by means of decryption keys that exhibit restricted availability.

The method is particularly advantageous since it can allow for the recordal and encryption of all communications traffic so that potentially incriminating traffic from a later-identified criminal source has already been recorded and the restricted availability of the decryption keys can then allow for a means for accessing the potentially incriminating communications evidence in a same controlled manner as known wire-taps are currently permitted.

Preferably, the method can be implemented employing spare disk space, and/or CPU capacity within a currently existing telecommunications system. This has the particular advantage of allowing for implementation of the method at negligible additional cost.

Also, the decryption keys arranged to be issued in a secure and authorised manner can be arranged to contain encrypted search conditions serving to restrict their scope of use. For example, a "where" clause can be embedded within the decryption key so as to allow access only to those encrypted data records that match the authorised search criteria.

Further, the decryption key can contain discreet levels of authorisation for access to the encrypted data.

According to a further advantage, the decryption keys can be arranged to be used only once so as to advantageously prevent unauthorised subsequent searches through the recorded data.

Advantageously, the method includes the steps of logging all attempted accesses to the stored data. This can advantageously provide for secure and encrypted audit trail accessible only by means of specially granted keys available only to reviewing/auditing bodies rather than, for example, law enforcement agencies.

According to a further feature, the method can provide for the inclusion of tamper detection reference data.

Advantageously, the method is arranged to record all communications traffic and to likewise store all of the recorded traffic.

In particular, the method is applicable to communications traffic through a node such as a telecommunications switch, router or gateway.

Preferably, the method also includes the step of encrypting details concerning the communications traffic, which details are then also stored.

It will therefore be appreciated that the present invention can advantageously provide for a method for use in the monitoring of communications traffic as noted above and including the step of restricting the availability of the decryption keys in accordance with, in particular, legislative requirements.

According to another aspect of the present invention, there is provided a system for use in the monitoring of communications traffic and including means for recording the said traffic, means for storing the recorded traffic as

encrypted data such that the data can be decrypted only by means of decryption keys that exhibits restricted availability.

The invention also preferably includes a system arranged to operate in accordance with the method steps outlined above.

The invention is described further hereinafter by way of example only, with reference to the accompanying drawing which comprises a schematic block diagram of a telecommunications monitoring system according to an embodiment of the present invention.

Turning now to the accompanying drawing, there is illustrated a telecommunications monitoring system 10 for monitoring communications traffic 12 travelling through, for example, a telecommunications switch 14. The system includes a recording device 16 that taps into the switch 14 so as to record all of the traffic passing there-through. The recorded traffic is then delivered to an encryption engine 18 which can employ any one or more of the appropriate currently available encryption schemes and in particular one or more of the 128-bit currently available encryption schemes.

The encrypted data is then delivered to the storage means 20 in which it can be stored for any appropriate amount of time, if not indefinitely, in accordance with legislative requirements. The encrypted data within the storage means 20 can be accessed and decrypted by means of decryption keys 22.

Typically, the available storage space can be recycled so as to provide a "first in first out" (FIFO) buffer of recordings which are retained for the maximum possible duration before being overwritten with more recent recordings.

However, an authorising system 24 is in place, which can be controlled by any appropriate authorising, or legislative body, such that the decryption keys 22 are only made available should specific criteria be met.

As an example, the decryption keys can be issued in a manner similar to currently existing schemes for authorising wire-taps.

The availability of so-called wire-tap warrants is currently closely controlled for example in the US by means of the Federal Communications Commission by means of the Communications Assistance for Law Enforcement Act 1994 whereas similar legislation has been introduced in the United Kingdom by means of the Regulation of Investigatory Powers Act 2000.

Such systems can advantageously allow for separate levels of authorisation such as the so-called "pen and trace" warrant or the "wire-tap" warrant controlled in the US under the above-mentioned Communication Assistance for Law Enforcement Act 1994.

Advantageously, the decryption keys can themselves contain encrypted search conditions so as to satisfactorily reduce, or eliminate, the chance of abuse and error. That is, if a warrant is issued to allow for the review of the calls only from one particular source, to one particular destination, or only calls within a particular time frame, appropriate clauses can be embedded within the decryption key so that only those encrypted records that match the quite specific criteria are made available.

Thus, as will be appreciated, and with particular reference to the enclosed drawing, the present invention provides for a particular advantageous concept in communications monitoring in which there is a no danger of important communications evidence being lost due to delays in seeking appropriate surveillance authorisation since the obtaining of such authorisation is time-shifted to a point at which the recording is made, and the

granting of the authorisation relates merely to accessing a secure recording thereof.

It should be appreciated that the present invention is not restricted to the details of the foregoing embodiments. For example, the concept can be applied to any appropriate form of communication, and indeed the communication of any appropriate data and whether comprising audio, modem, fax or data network packet data such that, for example, PC terminal activity can also be monitored for subsequent review if authorised.

With regard to realisation of the concept it should be noted that telephone switch manufacturers could readily embed the capability of recording all calls in next generation switches for a few percent of the total cost of the system.

All calls could be recorded using heavy-weight encryption so as to maintain public confidence that the same controls were in place to grant access to recordings that are used today to authorise wire-tapping, i.e. decryption keys are only issued as a warrant is granted. Initially it may only be viable to retain such recordings for a few days although increasingly inexpensive storage capabilities will assist in increasing such periods.

This capability could be added to every cellular base station, every central office switch and every corporate switch.

The ability to go back through all calls made after the event by identified terrorists can have a significant effect on follow-up operations.

Whilst the concept of the wire-tapping of telephone lines is well known, the use of a PC can also be monitored.

For example, while programmers first introduced "log files" into specific applications as diagnostic aids to help them understand how someone broke their program, and from the concept of being able to note everything that happened on a PC goes back to the venerable tools like "PC Anywhere" it was a fairly small step from there to keeping a log file of everything that happened on the screen during your session.

More recently, this concept has been increasingly used in call centres to review maybe 1% of calls to see how customer service reps are using the computer system during phone calls.

Increasing amounts of business are conducted on mixed channels – with a caller on the line also looking at his browser where a staff member is highlighting terms and conditions on a competitor's web-site. Regulatory bodies have only just began to be aware of potential loop-holes in rules that insist on voice recording only. Where communication involves multiple channels it is vital that all channels are recorded together, archived together and replayable together.

Claims

1. A method for use in the monitoring of communications traffic, comprising the step of recording the said traffic and storing the recorded traffic in an encrypted data format such that the data can be decrypted only by means of keys that exhibit restricted availability.

2. A method as claimed in Claim 1 and arranged to employ a spare disk and/or CPU capacity within a telecommunications system.

3. A method as claimed in Claim 1 or 2 and including the step of including encrypted search conditions within the decryption keys that are made selectively available.

4. A method as claimed in Claim 1, 2 or 3, and including the step of employing separate levels of authorisation for access to the stored data.

5. A method as claimed in any one or more of Claims 1-4, and including the step of employing a decryption key that is useable only once.

6. A method as claimed in any one or more of the preceding claims, and including the step of logging all accesses to the stored data to an encrypted secure audit trail.

7. A method as claimed in any one or more of the preceding claims and including a tamper detection reference within the encrypted data.

8. A method as claimed in any one or more of the preceding claims, and including the step of monitoring all the available communications traffic.

9. A method as claimed in Claim 8 and when the step of storing the recorded traffic comprises the step of recording all of the recorded traffic.

10. A method as claimed in any one or more of the preceding claims, wherein the communications traffic to be recorded comprises traffic through a telecommunications switch, router or gateway.

11. A method as claimed in any one or more of the preceding claims, and including the step of encrypting details relating to the communications traffic and storing the said encrypted details for subsequent access.

12. A method as claimed in any one or more of the preceding claims and including the step of authorising use of the required decryption key in a restricted manner.

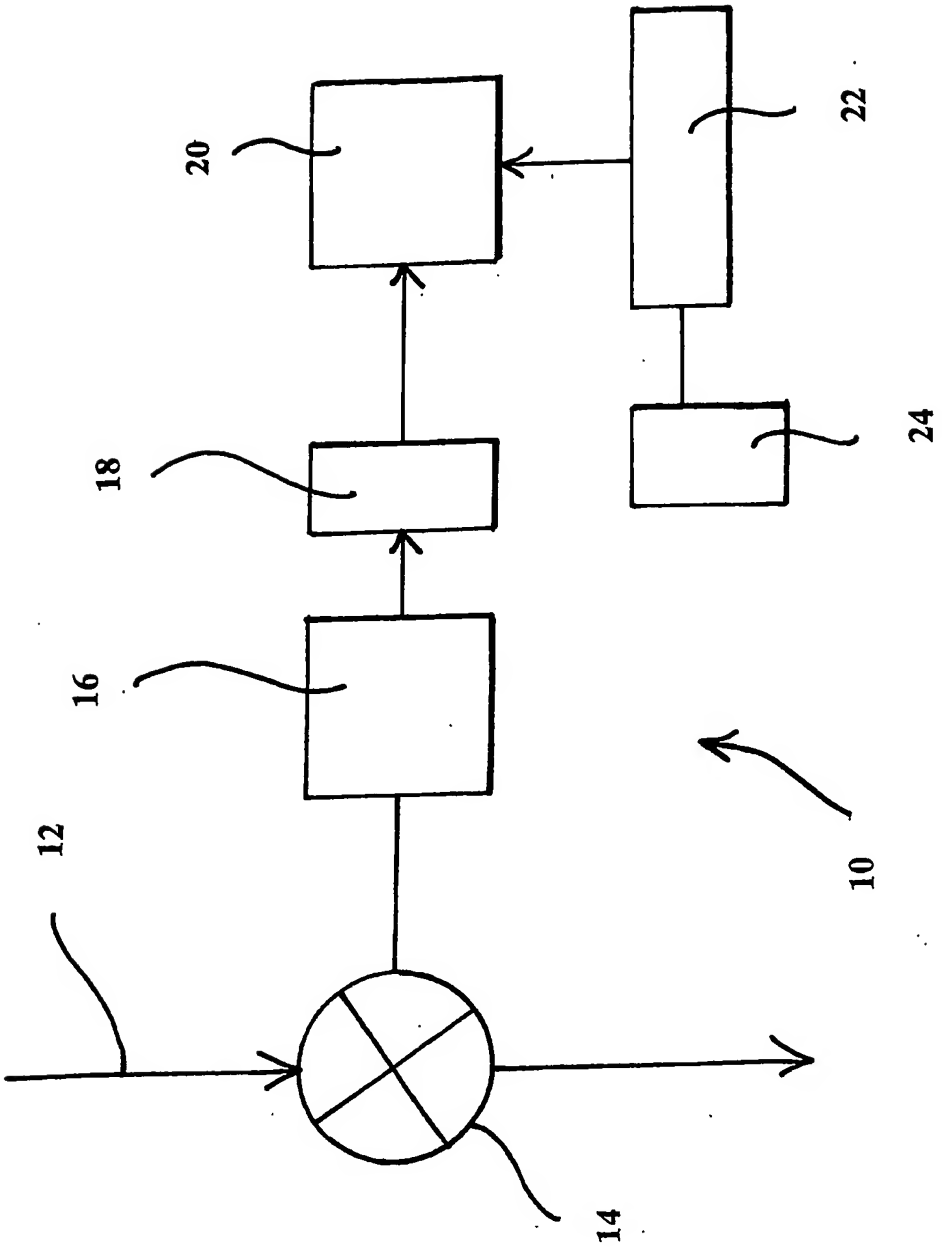
13. A system for use in the monitoring of communications traffic, including means for recording the said traffic and means for storing the recorded traffic as encrypted data, such that the recorded data can be decrypted only by means of keys that exhibit restricted availability.

14. A system as claimed in Claim 13 and arranged with means for executing the method steps of any one or more of Claims 2-12.

15. A method for use in the monitoring of telecommunications traffic substantially as hereinbefore described with reference to, and as illustrated in the accompanying drawing.

16. A system for use in the monitoring of telecommunications traffic substantially as hereinbefore described with reference to, and as illustrated in the accompanying drawing.

1/1



INTERNATIONAL SEARCH REPORT

Internati . . plication No
PCT/GB 03/03668

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F1/00 H04M3/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	C.J. ANTONELLI, P. HONEYMAN: "Wiretapping the internet" SPIE SYMPOSIUM ON ENABLING TECHNOLOGIES FOR LAW ENFORCEMENT AND SECURITY, HELD ON 5 NOV 2000, RETRIEVED FROM INTERNET, WWW.SPIEDL.COM, vol. 4232, February 2001 (2001-02), pages 75-84, XP002262366 page 75 -page 78 ---	1,2,4-6, 8-14
A	US 5 414 771 A (FAWCETT JR KENNETH J) 9 May 1995 (1995-05-09) column 2, line 29-45 -----	1,5

☐ Further documents are listed in the *continuation of box C.*

☒ Patent family members are listed in annex.

* Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the International search	Date of mailing of the international search report
21 November 2003	02/12/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Hes, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/GB 03/03668

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 3,7,15,16
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 3,7,15,16

The wording of claims 3, 7, 15 and 16 is such that a lack of clarity within the meaning of PCT Article 6 arises to such an extent as to render a meaningful search of these claims impossible.

Consequently, the search has been carried out for those parts of the application which do appear to be clear, namely Claims 1, 2 , 4-6, 8-14.

The applicant's attention is drawn to the fact that claims, or parts of claims, relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure.

INTERNATIONAL SEARCH REPORT

Internat ...plication No
PCT/GB 03/03668

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5414771 A	09-05-1995	NONE	